Claims:

Sub a1

1. A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein the security monitoring means further comprises means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts.

2. The system of Claim 1, wherein the detecting means further comprises means for storing a copy of the mobile application when the mobile application first passes through the server, means for receiving the mobile application after it is executed by another host and means for comparing the code of the mobile application after it is executed by another host to the stored copy of the mobile application to determine if changes have been made to the code of the mobile application.

3. A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein the security monitoring means further comprises means for preventing a host from transmitting hostile code in a mobile application to another host.

4. The system of Claim 3, wherein the preventing means further comprises means for determining if the host dispatching the mobile application is trusted, means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code of the mobile application, and means, when requested by another host, for providing the code for the mobile application to the requesting host.

5. A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein security monitoring means further comprises means for detecting unwanted changes in the state of the mobile application.

6. The system of Claim 5, wherein the detecting means further comprises means for saving a copy of the state of a received mobile application, means for receiving the same mobile application after a jump to another host and means for comparing the state of the mobile

application after the jump to another host with the stored state of the mobile application to ensure that the state of the mobile application has not changed.

7. A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein the security monitoring means further comprises means for detecting unwanted changes in the itinerary of the mobile application.

8. The system of Claim 7, wherein the detecting means further comprises means for saving a copy of the itinerary of a received mobile application, means for receiving the same mobile application after a jump to another host and means for comparing the itinerary of the mobile application after the jump to another host with the stored itinerary of the mobile application to ensure that the itinerary of the mobile application has not changed.

9. The system of Claim 7, wherein the itinerary comprises past historical itinerary data.

10. A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts.

11. The method of Claim 10, wherein the detecting further comprises storing a copy of the mobile application when the mobile application first passes through the server, receiving the mobile application after it is executed by another host and comparing the code of the mobile application after it is executed by another host to the stored copy of the mobile application to determine if changes have been made to the code of the mobile application.

12. A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises preventing a host from transmitting hostile code in a mobile application to another host.

13. The method of Claim 12, wherein the preventing further comprises determining if the host dispatching the mobile application is trusted, stripping the code from an initially received mobile application if the host is not trusted, saving the code of the mobile application, and, when requested by another host, providing the code for the mobile application to the requesting host.

14. A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises detecting unwanted changes in the state of the mobile application.

15. The method of Claim 14, wherein the detecting further comprises saving a copy of the state of a received mobile application, receiving the same mobile application after a jump to another host and comparing the state of the mobile application after the jump to another host with the stored state of the mobile application to ensure that the state of the mobile application has not changed.

16. A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises detecting unwanted changes in the itinerary of the mobile application.

17. The method of Claim 16, wherein the detecting further comprises saving a copy of the itinerary of a received mobile application, receiving the same mobile application after a jump to another host and comparing the itinerary of the mobile application after the jump to another host with the stored itinerary of the mobile application to ensure that the itinerary of the mobile application has not changed.

18. The method of Claim 16, wherein the itinerary comprises past historical itinerary data.

19. A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises preventing untrusted hosts from initially launching mobile applications